UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/559,889	12/07/2005	Junbiao Zhang	PU030227	2851

24498 7590 10/01/2008

Joseph J. Laks
Thomson Licensing LLC
2 Independence Way, Patent Operations
PO Box 5312
PRINCETON, NJ 08543

EXAMINER	
NGUYEN, TRONG H	
ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
10/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/559,889	ZHANG ET AL.	
	Examiner	Art Unit	
	TRONG NGUYEN	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) *2* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-14* is/are rejected.

7)☒ Claim(s) *1,3-6 and 8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/07/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The instant application numbered 10559889 filed on 12/07/2005 is presented for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63**.

Priority

3. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged.

Drawings

4. The applicant's submitted drawings are acceptable for examination purposes.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 12/07/2005 is in compliance with the provisions of 37 C.R.R. 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

6. The disclosure is objected to because of the following informalities: Page 6, line 16 recites "starup" which appears to be a misspelling of "startup".

Appropriate correction is required.

Claim Objections

7. Claim **1** is objected to because of the following informalities: Claim **1**, line 7 recites "the newly generated encryption key" which appears to be referred to "new encryption key" in line 6 and therefore is inconsistent. Appropriate correction is required.

Claim **3** is objected to because of the following informalities: Claim **3**, line 20 recites "said decrypting" which appears to be referred to "decryption failure" in claim **1**, line 12 and thus is inconsistent. Furthermore, claim **3**, line 21 recites "the station encryption key" which appears to be referred to "encryption key being used by the station" in claim **1**, line 8 and hence is inconsistent. In addition, claim **3**, line 21 recites "the current key" which appears to be referred to "current encryption key" and thus is inconsistent. Appropriate correction is required.

Claim **4** is objected to because of the following informalities: Claim **4**, lines 26-29 recites "the new key" which appears to be referred to "new encryption key" in line 6 of claim **1** and hence is inconsistent. Furthermore, line 30 recites "the old key" and "the current key" which appears to be referred to "old encryption key" and "current encryption key" in claim **1** respectively and thus is inconsistent. Appropriate correction is required.

Claims **5, 6,** and **8** are objected to because of the following informalities: Claim **5**, line 1 recites "the old key" which appears to be referred to "old encryption key" in claim **1** and hence is inconsistent. Claim **6**, line 4 recites "the current key" which appears to be referred to "current encryption key" in claim **1** and thus is inconsistent. Claim **8**, line 15 recites "said new key" which appears to be referred to "new encryption key" and therefore is inconsistent. Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims **6** and **14** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim **6** recites the limitation "the first key" in line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim **14** recites the limitation "the termination of communication" in line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claim **8** is rejected under 35 U.S.C. 102(b) as being anticipated by Lewis US 6,526,506 (hereinafter "Lewis").

Lewis discloses **"A key synchronization mechanism for a wireless network comprising:"** [the access point generates a new ENCRYPT key to be use as the current ENCRYPT key (Col. 12, lines 43-44), transmits the new ENCRYPT key to the mobile terminal (Col. 12, lines 44-46), and determines if the message received from the mobile terminal has been encrypted using the current ENCRYPT key (Col. 12, line 67-Col. 13, lines 1-2)] **"at least one station in the wireless network;"** ["The wireless communication system 50 also includes one or more mobile terminals 66" (Fig. 1, Col. 4, lines 28-29)] **"and at least one access point in the wireless network** ["Connected to the system backbone 52 are several access points 54" (Fig. 1, Col. 4, lines 14-15)] **maintaining an old encryption key** [previous ENCRYPT key (Col. 6, line 57) **and a new encryption key through a key rotation interval for each of said at least one station** [Periodically, the access point may be instructed to use a different or new ENCRYPT key (Col. 12, lines 43-44) and the new ENCRYPT key is transmitted to the mobile terminal (Col. 12, lines 44-46)] **"said access point using said new encryption key when a first data frame correctly encrypted with said new key is received from said at least one station"** [If the message is encrypted using the current ENCRYPT key as determined in step 222, the access point decrypts the message (Lewis, Fig. 7, Col. 13, lines 8-9). Furthermore, by disclosing when it is determined that the message received is not encrypted using the current ENCRYT key, the access point

does not decrypt the message but proceeds to step 226 (Lewis, Fig. 7, Col. 13, lines 13-15, 34-35), Lewis also discloses the access point starts using the new ENCRYPT key when a first message is correctly encrypted under the new ENCRYPT key by the mobile terminal] "**and using said old encryption key when decryption of a data frame received from said at least one station fails due to mismatched keys**" [By disclosing the access point using the previous ENCRYPT key to encrypt the new ENCRYPT key before transmitting it to the mobile terminal (Col. 12, lines 44-46), Lewis also discloses using the previous key in encrypting and decrypting messages. Furthermore, Lewis also discloses using a MASTER key to decrypt data packet received from the mobile terminal when there is a mismatch in encryption key (Col. 11, lines 49-51, 52-54, and 58-62). Hence, Lewis also discloses using an existing key (previous ENCRYPT key) in situation where the new ENCRYPT key is not valid due to mismatch.]

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims **1**, **7**, and **13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Raith US 5,241,598 (hereinafter "Raith").

Regarding claim **1**, Lewis discloses "**A key synchronization method for a wireless network comprising:**" as [the access point generates a new ENCRYPT key to be use as the current ENCRYPT key (Col. 12, lines 43-44), transmits the new ENCRYPT key to the mobile terminal (Col. 12, lines 44-46), and determines if the message received from the mobile terminal has been encrypted using the current ENCRYPT key (Col. 12, line 67-Col. 13, lines 1-2)] "**setting a current encryption key** [ENCRYPT key (Col. 6, line 46)] **and an old encryption key** [previous ENCRYPT key (Col. 6, line 57)] **at an access point** [an access point 54 (Col. 6, line 55)] **in the wireless network**;" [wireless network (Col. 1, line 26)] "**generating a new encryption key at the access point**" as [Periodically, the access point may be instructed to use a different or new ENCRYPT key (Col. 12, lines 43-44)] "**communicating the new encryption key to the station in an encrypted form using the old encryption key**;" as [The access point communicates the new ENCRYPT key using the previous ENCRYPT key (Col. 12, lines 44-46)] "**indicating a decryption failure for a data frame received from the station when the encryption key used by the station does not match the current encryption key**" as [Fig. 7, access point determines if the message from received from the mobile terminal is encrypted with the current ENCRYPT key, if not, the access point follows appropriate actions described in steps 226-234] "**wherein a data frame that failed to decrypt using the current encryption key is decrypted using the old encryption key**" as [By disclosing the access point using the previous ENCRYPT key to encrypt the new ENCRYPT key before transmitting it to the mobile terminal (Col. 12, lines 44-46), Lewis also discloses using the previous

key in encrypting and decrypting messages. Furthermore, Lewis also discloses using a MASTER key to decrypt data packet received from the mobile terminal when there is a mismatch in encryption keys (Col. 11, lines 49-51, 52-54, and 58-62). Hence, Lewis also discloses using an existing key (previous ENCRYPT key) in situation where the new ENCRYPT key is not valid due to mismatch.]

Lewis does not specifically disclose **"resetting the current encryption key to equal the newly generated encryption key;"** and **"resetting the old encryption key to equal an encryption key being used by a station in communication with the access point."**

However, Raith discloses a method and apparatus for resynchronizing a rolling key used in the validation and verification of base stations and mobile stations within a cellular radio communications system" (Col. 1, lines 32-35) wherein the current encryption key ($S\text{-}key_{s\text{-}p}$) is reset to equal the new encryption key ($S\text{-}key\text{-}next_{s\text{-}p}$) (Col. 34, lines 44-45), the old encryption key ($S'\text{-}key_s$) is reset to equal the current encryption key being used by the mobile terminal in communication with the access point ($S\text{-}key_{s\text{-}p}$) (Col. 34, lines 64-65).

Raith and Lewis are analogous art because they are in the same field of endeavor of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Lewis's key synchronization method by having the access point resets the current ENCRYPT key to equal the new ENCRYPT key and resets the previous ENCRYPT key equal the current ENCRYPT key as described by Raith in order

to "alleviate the security concerns engendered by radio transmission of confidential data" (Raith, Col. 4, lines 38-40).

Regarding claim **7**, Lewis in view of Raith discloses "**The method according to claim 1, wherein said step of setting is performed by the access point for each station in the wireless network**" as [see rejection to claim **1** above.]

Regarding claim **13**, Lewis in view of Raith discloses "**The method according to claim 1, wherein the new encryption key is generated at the access point upon expiration of a key refresh interval**" as [Periodically, the access point may be instructed to use a different or new ENCRYPT key (Lewis, Col. 12, lines 43-44).]

13. Claims **3**, **4**, and **14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Raith and further in view of Loc et al. US 7,293,289 (hereinafter "Loc").

Regarding claim **3**, Lewis in view of Raith discloses "**The method according to claim 1, further comprising:**" and "**decrypting received data frames associated with said out-of-sync counter at the access point using the old encryption key**" [see rejection to claim **1** above] but does not specifically disclose "**incrementing an out-of-sync counter in the access point when said decrypting fails due to the station encryption key not matching the current key.**"

However, Loc discloses a method for detecting a security breach in a network wherein "Each time a client 108 fails to successfully decrypt a packet, the encryption failure counter is incremented" (Fig. 5, Col. 6, lines 59-61).

Loc, Lewis, and Raith are analogous art because they are in the same field of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the key synchronization method of Lewis in view of Raith by including a counter at the access point which is incremented after a decryption failure due to mismatched encryption keys as described by Loc in order to detect a security breach in a network (Loc, Col. 1, lines 22-23).

Regarding claim **4**, Lewis in view of Raith discloses "**The method according to claim 1, further comprising: decrypting, using the new key, the received data frame from the station when the access point determines the station sending the received packet is using the new key, said access point starting to use the new key when a first data frame correctly encrypted with the new key is received from the station;**" as [If the message is encrypted using the current ENCRYPT key as determined in step 222, the access point 54 decrypts the message (Lewis, Fig. 7, Col. 13, lines 8-9). Furthermore, by disclosing when it is determined that the message received is not encrypted using the current ENCRYT key, the access point does not decrypt the message but proceeds to step 226 (Lewis, Fig. 7, Col. 13, lines 13-15, 34-35), Lewis also makes it obvious that the access point starts using the new ENCRYPT key when a first message is correctly encrypted under the new ENCRYPT key by the mobile terminal] "**re-setting the old key to equal the current key when decryption is successful;** as [With respect to this limitation, by disclosing upon unsuccessful authentication which occurs when the access point and the mobile station does not

have the same enciphering key (Raith, Col. 22, lines 53-55), ciphering key value stored in the second location (S-key_{s-p} or current key) is set to the ciphering key value stored in the fourth location (S'-key_s or old encryption key) (Raith, Col. 8, lines 10-12, 19-22, 42-45, and 50-53), Raith also makes it obvious to set the old encryption key to equal the current encryption key upon successful authentication] but does not specifically disclose **"and re-setting an out-of-sync counter to zero upon successful decryption**".

However, Loc discloses a method for detecting a security breach in a network wherein "Each time client 108 successfully decrypts a packet, the encryption failure counter is reset to zero" (Loc, Col. 6, lines 57-69).

Loc, Lewis, and Raith are analogous art because they are in the same field of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the key synchronization method of Lewis in view of Raith by including a counter at the access point which is incremented after a decryption failure due to mismatched encryption keys and is reset to zero after a successful decryption as described by Loc in order to detect a security breach in a network (Loc, Col. 1, lines 22-23).

Regarding claim **14**, for examining purposes, "the termination of communication" will be considered as "a termination of communication". Lewis in view of Raith and further in view of Loc discloses "**The method according to claim 3, wherein said out-of-sync counter comprises a predetermined threshold that if exceeded causes the termination of communication between the access point and a source of the data**

frames causing the threshold of said out-of-sync counter to be exceeded" as ["When the encryption failure counter reaches a predetermined threshold n (that is, when n consecutive failures have occurred) (step 512), client 108 sends an alert packet to access point" (Loc, Col. 6, lines 61-65). Furthermore, upon receiving the alert of a security breach, the access point "responds by immediately removing the MAC address of client 108 from its list of authorized clients, by ceasing to send any packets to the MAC address of client 108, and by discarding all packets that are received from the MAC address of client 108" (Loc, Col. 6, lines 5-9).]

14. Claims **5** and **6** are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Raith and further in view of Kelem et al. US 6,118,869 (hereinafter "Kelem").

Regarding claim **5**, Lewis in view of Raith discloses **"The method according to claim 1"** but does not specifically disclose **"further comprising setting the old key equal to a null value, said null value representing a no encryption mode"**.

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Lewis, and Raith are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the key synchronization method of Lewis in view of Raith by setting a key or in this case, the old ENCRYPT key to a null value which represents a no encryption mode as taught by Kelem in order to provide a high level of security (Kelem, Col. 2, lines 10-14).

Regarding claim **6**, for examining purposes, "the first key" will be considered as "the new encryption key". Lewis in view of Raith discloses "**The method according to claim 1, further comprising**" but does not specifically disclose "**setting the current key and the first key to a null value, said null value representing a no encryption mode**".

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Lewis, and Raith are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the key synchronization method of Lewis in view of Raith by setting a key or in this case, the current ENCRYPT key and the new ENCRYPT key to a null value which represents a no encryption mode as taught by Kelem in order to provide a high level of security (Kelem, Col. 2, lines 10-14).

15. Claim **9** is rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Loc.

Lewis discloses "**The key synchronization mechanism according to claim 8**" but does not specifically disclose "**wherein said at least one access point further maintains an out-of-sync counter to track the number of packets where decryption fails due to mismatched keys**".

However, Loc discloses a method for detecting a security breach in a network wherein "Each time client 108 fails to successfully decrypt a packet, the encryption failure counter is incremented" (Fig. 5, Col. 6, lines 59-61).

Loc and Lewis are analogous art because they are in the same field of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Lewis's key synchronization method by including an encryption failure counter at the access point which keeps track of the number of packets that were not successfully decrypted due to mismatched keys as described by Loc in order to detect a security breach in a network (Loc, Col. 1, lines 22-23).

16. Claims **10**, **11**, and **12** are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Kelem.

Regarding claim **10**, Lewis discloses "**The key synchronization mechanism according to claim 8**," but does not specifically disclose "**wherein said at least one**

access point is capable of setting the old encryption key to a null value, said null value representing a no encryption mode".

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem and Lewis are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the key synchronization method of Lewis by setting a key at the access point or in this case, the old ENCRYPT key to a null value which represents a no encryption mode as taught by Kelem in order to provide a high level of security (Kelem, Col. 2, lines 10-14).

Regarding claim **11**, Lewis discloses "**The key synchronization mechanism according to claim 8**," but does not specifically disclose "**wherein said at least one access point is capable of setting the new encryption key to a null value, said null value representing a no encryption mode**".

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem and Lewis are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the key synchronization method of Lewis by setting a key at the access point or in this case, the new ENCRYPT key to a null value which represents a no encryption mode as taught by Kelem in order to provide a high level of security (Kelem, Col. 2, lines 10-14).

Regarding claim **12**, Lewis discloses "**The key synchronization mechanism according to claim 8**," but does not specifically disclose "**wherein said at least one access point initially sets the old encryption key to a null value**".

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem and Lewis are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the key synchronization method of Lewis by setting a key at the access point or in this case, the old ENCRYPT key initially to a null value which represents a no encryption mode as taught by Kelem in order to provide a high level of security (Kelem, Col. 2, lines 10-14).

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US 2003/0221098

US 4,972,472

US 5,706,348

US 7,400,733

US 2003/0219129

US 6,377,692

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRONG NGUYEN whose telephone number is (571)270-7312. The examiner can normally be reached on Monday through Thursday 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on (571)272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TN

/Thomas K Pham/
Supervisory Patent Examiner, Art Unit 4148